

Tschirnhausen transformation of a cubic generic polynomial and a 2-dimensional involutive Cremona transformation

By Akinari HOSHI*) and Katsuya MIYAKE**)

To the memory of Professor Shokichi Iyanaga

(Communicated by Heisuke HIRONAKA, M.J.A., March 12, 2007)

Abstract: We study the field isomorphism problem for a cubic generic polynomial $X^3 + sX + s$ via Tschirnhausen transformation. Through this process, there naturally appears a 2-dimensional involutive Cremona transformation. We show that the fixed field under the action of the transformation is purely transcendental over an arbitrary base field.

Key words: Tschirnhausen transformation; cubic generic polynomial; field isomorphism problem; involutive Cremona transformation; general Noether problem.

1. Introduction. Let k be a field whose characteristic $\text{ch}(k)$ is different from 3 and which may not be algebraically closed. Let $k(s)$ be the rational function field over k with an indeterminate s . In this paper, we study the cubic polynomial $R(s; X) := X^3 + sX + s \in k(s)[X]$. We denote by $\text{Spl}_k f(X)$ the splitting field of a polynomial $f(X) \in k[X]$ over a field k . The polynomial $R(s; X)$ is well-known as a k -generic S_3 -polynomial (cf. e.g. [6, 9, 15]). Namely the Galois group of $R(s; X)$ over $k(s)$ is isomorphic to the symmetric group S_3 of degree 3 and every S_3 -Galois extension $L/K \supset k$ can be obtained as $L = \text{Spl}_K R(c; X)$ for some $c \in K$ (see [7]). Note that from Kemper's Theorem [8] every C_2 - or C_3 -Galois extension L'/K which includes a base field k also can be realized as $L' = \text{Spl}_K R(d; X)$ for some $d \in K$. Conversely, in the case of $k = \mathbf{Q}$, there exist one-parameter \mathbf{Q} -generic polynomials only for the groups C_2, C_3 and S_3 (cf. [7, 12]).

We shall treat the field isomorphism problem for $R(s; X)$ via general Tschirnhausen transformation. Indeed in Section 2, we show that

Theorem (Theorem 1). *Let $M \supseteq K \supseteq k(s)$ be a tower of fields, and $R(s; X) = X^3 + sX + s \in K[X]$. For $s' \in K, (s' \neq s)$, the following two statements are equivalent:*

(i) $\text{Spl}_M R(s'; X) = \text{Spl}_M R(s; X)$;

(ii) *there exists an element $u \in M$ such that*

$$s' = \frac{s(u^2 + 9u - 3s)^3}{(u^3 - 2su^2 - 9su - 2s^2 - 27s)^2}.$$

As a consequence of Theorem 1, we give a necessary and sufficient condition of $\text{Spl}_k R(c; X) = \text{Spl}_k R(d; X)$ for $c, d \in k$.

Under the condition of the theorem, there also exists $u' \in M$ such that

$$s = \frac{s'(u'^2 + 9u' - 3s')^3}{(u'^3 - 2s'u'^2 - 9s'u' - 2s'^2 - 27s')^2}.$$

Then by these formulas for s and s' , we are able to determine u and u' as

$$u = -\frac{(u'^2 + 3s')(u'^2 + 9u' - 3s')}{u'^3 - 2s'u'^2 - 9s'u' - 2s'^2 - 27s'},$$

$$u' = -\frac{(u^2 + 3s)(u^2 + 9u - 3s)}{u^3 - 2su^2 - 9su - 2s^2 - 27s}.$$

Hence we obtain a 2-dimensional involutive Cremona transformation σ over an arbitrary field k' . Indeed, let S and U be two independent variables over a field k' of any characteristic, and define $\sigma \in \text{Cr}_2(k') = \text{Aut}_{k'}(k'(S, U))$ by

$$\sigma : (S, U) \mapsto \left(\frac{S(U^2 + 9U - 3S)^3}{(U^3 - 2SU^2 - 9SU - 2S^2 - 27S)^2}, \right. \\ \left. - \frac{(U^2 + 3S)(U^2 + 9U - 3S)}{U^3 - 2SU^2 - 9SU - 2S^2 - 27S} \right).$$

Involutive Cremona birational transformations were classically studied by geometers in the so-called Italian school, for examples, E. Bertini [1] and G. Castelnuovo and F. Enriques [5]. Recently, L. Bayle and A. Beauville [2] gave a complete classification

2000 Mathematics Subject Classification. 12F12, 12F20, 14E07, 14E08.

*) Department of Mathematics, School of Education, Waseda University, 1-6-1 Nishi-Waseda, Shinjuku-ku, Tokyo 169-8050, Japan.

***) Department of Mathematical Sciences, School of Science and Engineering, Waseda University, 3-4-1, Ohkubo, Shinjuku-ku, Tokyo 169-8555, Japan.

of conjugacy classes of the 2-dimensional involutions over an algebraically closed field with characteristic not equal 2; their method is based on investigation of biregular involutions of rational surfaces under the Mori theory.

In our present work, we encountered the above involutive Cremona transformation σ which is definable over an arbitrary base field even with characteristic 2.

We solve the rationality problem for $k'(S, U)^{(\sigma)}$ and obtain Zariski-Castelnuovo's theorem (cf. [17]) by constructing a minimal basis for $k'(S, U)^{(\sigma)}$.

Theorem (Theorem 10). *Let k' be a field. The fixed field $k'(S, U)^{(\sigma)}$ of $k'(S, U)$ under the action of σ is purely transcendental over k' . If $\text{ch}(k') \neq 2$ then a minimal basis for $k'(S, U)^{(\sigma)}$ is given as*

$$k'(S, U)^{(\sigma)} = k' \left(\frac{2SU^3 + 9U^3 + 9SU^2 + 2S^2U + 54SU - 9S^2}{U^3 - 2SU^2 - 9SU - 2S^2 - 27S}, \frac{S(4S + 27)(U^2 + 9U + S + 27)}{(2U + 9)(U^3 - 2SU^2 - 9SU - 2S^2 - 27S)} \right).$$

If $\text{ch}(k') = 2$ then

$$k'(S, U)^{(\sigma)} = k' \left(\frac{U^3 + SU^2 + S^2}{U^3 + SU + S}, \frac{S}{U^3 + SU + S} \right).$$

2. Tschirnhausen transformation. Generally speaking, let $f(X), g(X) \in k[X]$ be monic polynomials of degree n over a field k , and let $\{\alpha_i\}_{1 \leq i \leq n}$ and $\{\beta_i\}_{1 \leq i \leq n}$ be the roots of $f(X)$ and $g(X)$ in a fixed algebraic closure of k , respectively. A polynomial $g(X)$ is called Tschirnhausen transformation of $f(X)$ over k , if there exist $c_0, \dots, c_{n-1} \in k$ such that

$$g(X) = \prod_{i=1}^n \left(X - \sum_{j=0}^{n-1} c_j \alpha_i^j \right).$$

Two polynomials $f(X)$ and $g(X)$ in $k[X]$ are Tschirnhausen equivalent over k , which is denoted $f(X) \sim_k g(X)$, if they are Tschirnhausen transformations over k of each other. The following three conditions are equivalent: (i) $f(X) \sim_k g(X)$, (ii) $k[X]/(f(X))$ and $k[X]/(g(X))$ are k -isomorphic, (iii) $k(\alpha_i) = k(\beta_j)$ for some $i, j, 1 \leq i, j \leq n$. Hence if we have $f(X) \sim_k g(X)$ then $\text{Spl}_k f(X) = \text{Spl}_k g(X)$. However the converse does not hold in general (e.g. $\text{Gal}(f(X)) \cong D_4, \text{PSL}_2(\mathbf{F}_7)$). In the case of $n = 3$, we see that $f(X) \sim_k g(X)$ if and only if $\text{Spl}_k f(X) = \text{Spl}_k g(X)$ because all subgroups of S_3 with index 3

are conjugate in S_3 . Furthermore, the following fact is known (cf. [3]): Let $f(X), g(X) \in k[X]$ be irreducible polynomials of prime degree with solvable Galois groups. Then $f(X) \sim_k g(X)$ if and only if $\text{Spl}_k f(X) = \text{Spl}_k g(X)$.

Now let $M \supseteq K \supseteq k(s)$ be a tower of fields. We define a 3×3 matrix Ξ over K as in [14, 15] by

$$\Xi := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -s & -s & 0 \end{pmatrix} \in M_3(K).$$

The cubic polynomial $R(s; X) := X^3 + sX + s \in K[X]$ is the characteristic polynomial of Ξ , and its discriminant is $-s^2(4s + 27)$. For $x, y, z \in M$, we put $\Xi' := xI_3 + y\Xi + z\Xi^2$, namely,

$$\Xi' := \begin{pmatrix} x & y & z \\ -sz & x - sz & y \\ -sy & -sy - sz & x - sz \end{pmatrix} \in M_3(M).$$

The characteristic polynomial $R'(x, y, z, s; X)$ of Ξ' is given by

$$\begin{aligned} (1) \quad R'(x, y, z, s; X) &= X^3 - (3x - 2zs)X^2 + (3x^2 + y^2s - 4xzs \\ &\quad + 3yzs + z^2s^2)X - x^3 - xy^2s + y^3s \\ &\quad + 2x^2zs - 3xyzs - xz^2s^2 + yz^2s^2 - z^3s^2. \end{aligned}$$

The polynomial $R'(x, y, z, s; X) \in M[X]$ is a general form of Tschirnhausen transformations of $R(s; X)$ over M . We can also obtain it as

$$\begin{aligned} R'(x, y, z, s; X) &= \text{Resultant}_Y(R(s; Y), X - (x + yY + zY^2)). \end{aligned}$$

Let $f_3(X)$ be a cubic polynomial in $K[X]$, and suppose that

$$\text{Spl}_M f_3(X) = \text{Spl}_M R(s; X) \quad \text{for } M \supseteq K.$$

Then there exist $x, y, z \in M$ such that $f_3(X) = R'(x, y, z, s; X)$. From now on, we consider the special case where $f_3(X) = R(s'; X) = X^3 + s'X + s'$, $s' \in K$. From (1), we have

$$\begin{aligned} 3x - 2zs &= 0, \\ 3x^2 + y^2s - 4xzs + 3yzs + z^2s^2 &= -x^3 - xy^2s \\ &\quad + y^3s + 2x^2zs - 3xyzs - xz^2s^2 + yz^2s^2 - z^3s^2. \end{aligned}$$

Hence we obtain

$$(2) \quad x = \frac{2zs}{3},$$

$$27y^2 - 27y^3 + 81yz + 18y^2zs - 9z^2s + 27yz^2s + 27z^3s + 2z^3s^2 = 0.$$

If $z = 0$ then we must have $(x, y) = (0, 1)$ and $R'(0, 1, 0, s; X) = R(s; X)$. Thus we assume $z \neq 0$, and put $u := 3y/z$; then from (2) we see

$$z^2(-9s + 27u + 3u^2 + 27zs + 2zs^2 + 9uzs + 2u^2zs - u^3z) = 0.$$

Hence we have

$$z = \frac{3(u^2 + 9u - 3s)}{u^3 - 2su^2 - 9su - 2s^2 - 27s}.$$

This means that, if $R'(x, y, z, s; X) = R(s'; X)$, ($s' \neq s$), then there exists $u \in M$ such that

$$(3) \quad (x, y, z) = \left(\frac{2sZ}{3}, \frac{uZ}{3}, Z \right), \text{ where}$$

$$Z = \frac{3(u^2 + 9u - 3s)}{u^3 - 2su^2 - 9su - 2s^2 - 27s}.$$

By a direct calculation, we have

$$R' \left(\frac{2sZ}{3}, \frac{uZ}{3}, Z, s; X \right)$$

$$= X^3 + \frac{s(u^2 + 9u - 3s)^3}{(u^3 - 2su^2 - 9su - 2s^2 - 27s)^2} (X + 1).$$

Hence we have obtained the following theorem.

Theorem 1. *Let $M \supseteq K \supseteq k(s)$ be a tower of fields. For $s' \in K$, ($s' \neq s$), the following two statements are equivalent:*

- (i) $\text{Spl}_M R(s'; X) = \text{Spl}_M R(s; X)$;
- (ii) *there exists an element $u \in M$ such that*

$$s' = \frac{s(u^2 + 9u - 3s)^3}{(u^3 - 2su^2 - 9su - 2s^2 - 27s)^2}.$$

3. Generic sextic polynomial.

In this Section, we consider the case of the rational function field $K = k(s, t)$ with two variables s, t over k . We assume that

$$\text{Spl}_M R(s; X) = \text{Spl}_M R(t; X) \quad \text{for } M \supseteq K$$

as in Theorem 1. With the equation of (ii) of Theorem 1 in mind, we define a sextic polynomial $F(s, t; X) \in K[X]$ by

$$F(s, t; X) := (s - t)X^6 + (4t + 27)sX^5$$

$$- (4st + 9s - 18t - 243)sX^4$$

$$- (32st + 162s - 54t - 729)sX^3$$

$$- (8st - 27s + 189t + 729)s^2X^2$$

$$- 9(4st - 27s + 54t)s^2X$$

$$- (4s^2t + 27s^2 + 108st + 729t)s^2.$$

If $X = u$ is a root of $F(s, t; X) = 0$, then t coincides with s' given in the above (ii). Let $\alpha_1, \dots, \alpha_6$ be the roots of $F(s, t; X)$ in a fixed algebraic closure of K . From Theorem 1, it follows that $\text{Spl}_M R(t; X) = \text{Spl}_M R(s; X)$ if and only if $F(s, t; X)$ has a root in M . The discriminant of $F(s, t; X) \in K[X]$ with respect to X is $(4s + 27)^{15}(4t + 27)^3 s^{10} t^4$. We put

$$L_s := \text{Spl}_K R(s; X), \quad L_t := \text{Spl}_K R(t; X).$$

Then we have $L_s \cap L_t = K$ and $\text{Gal}(L_s L_t / K) \cong S_3 \times S_3$.

Lemma 2. *Let $f(X) \in K[X]$ be a sextic polynomial with roots β_1, \dots, β_6 . The following conditions are equivalent:*

- (i) $L_s L_t = L_s(\beta_i) = L_t(\beta_i)$ for every $i, 1 \leq i \leq 6$;
- (ii) $f(X)$ is irreducible, $K(\beta_i) \subset L_s L_t$ and $L_s \cap K(\beta_i) = L_t \cap K(\beta_i) = K$ for every $i, 1 \leq i \leq 6$.

Proof. If $L_s L_t = L_s(\beta_i)$ then $K(\beta_i) \subset L_s L_t$, $[K(\beta_i) : K] = 6$ and $K(\beta_i) \cap L_s = K$. Similarly, we have $K(\beta_i) \cap L_t = K$. Conversely if the condition (ii) holds, then $[L_s(\beta_i) : L_s] = 6$ and $L_s L_t = L_s(\beta_i)$ for $i = 1, \dots, 6$. By the same way we have $L_s L_t = L_t(\beta_i)$. \square

As for our $F(s, t; X)$, we have $\text{Spl}_{K(\alpha_i)} R(s; X) = \text{Spl}_{K(\alpha_i)} R(t; X)$, that is $L_s(\alpha_i) = L_t(\alpha_i)$, and hence $L_s(\alpha_i) \supset L_s L_t$. Since $6 \geq [L_s(\alpha_i) : L_s] \geq [L_s L_t : L_s] = 6$, we have $L_s(\alpha_i) = L_s L_t$. Thus

Proposition 3. *The above defined sextic polynomial $F(s, t; X)$ and its roots $\alpha_1, \dots, \alpha_6$ satisfy the conditions (i) and (ii) of Lemma 2.*

Moreover we have

$$\text{Proposition 4.} \quad L_s L_t = K(\alpha_1, \dots, \alpha_6).$$

Proof. It follows from the previous proposition that

$$\text{Spl}_K F(s, t; X) = K(\alpha_1, \dots, \alpha_6)$$

$$\subseteq L_s L_t = \text{Spl}_K R(s; X) \cdot \text{Spl}_K R(t; X),$$

and $K(\alpha_1, \dots, \alpha_6) \not\subseteq L_s, K(\alpha_1, \dots, \alpha_6) \not\subseteq L_t$. However a normal subgroup N of $S_3 \times S_3$ which satisfies $N \not\subseteq 1 \times S_3$ and $N \not\subseteq S_3 \times 1$ must contain $C_3 \times C_3$ (for example, see [13]). Thus $[S_3 \times S_3 : N] \leq 4$. Hence $K(\alpha_1, \dots, \alpha_6)$ contains all of the cubic subextensions of L_s / K and L_t / K which generate $L_s L_t$. This shows the proposition. \square

The Galois group of the sextic polynomial $F(s, t; X)$ over K is isomorphic to ${}_6T_9$ ($\cong S_3 \times S_3$), the ninth transitive subgroup of S_6 (cf. [4]).

Theorem 5. *The sextic polynomial $F(s, t; X)$ ($\in k(s, t)[X]$) is a k -generic $(S_3 \times S_3)$ -polynomial.*

Proof. The assertion follows from Proposition 4 and S_3 -genericness of $R(s; X)$. \square

Remark 6. T. Komatsu [11] also obtained a sextic polynomial $P(s, t; X)$ satisfying the condition $\text{Spl}_K P(s, t; X) = \text{Spl}_K R(s; X) \cdot \text{Spl}_K R(t; X)$ as in Proposition 4 via descent Kummer theory (see also [10]). His paper [11] treats the subfield problem for $R(s; X)$ by using his $P(s, t; X)$.

4. Specialization of parameters. We consider the field isomorphism problem for $R(s; X)$. Put

$$L_c := \text{Spl}_k R(c; X), \quad L_d := \text{Spl}_k R(d; X),$$

for $c, d \in k$. Suppose $c, d \in k \setminus \{0, -27/4\}$. (Then the discriminant, $-s^2(4s+27)$, of $R(s; X)$ with respect to X does not vanish.) By specializing the parameters $(s, s') \mapsto (c, d) \in k^2$ in Theorem 1, we obtain an answer of the field isomorphism problem for $R(s; X)$ via Tschirnhausen transformation.

Theorem 7. *If $F(c, d; X)$ has an irreducible factor $f_n(X)$ of degree n over k , then a root field M of $f_n(X)$ satisfies $\text{Spl}_M R(c; X) = \text{Spl}_M R(d; X)$. Conversely, if there exists such an extension M of k with $[M : k] = n$, then $F(c, d; X)$ has an irreducible factor $f_m(X)$ of degree m with $m \mid n$ over k a root of which is contained in M .*

Corollary 8. *Two splitting fields L_c and L_d coincide if and only if $F(c, d; X)$ has a root in k .*

Example 9. We give some numerical examples for Theorem 7 over $k = \mathbf{Q}$. We put $G_c := \text{Gal}(L_c/\mathbf{Q})$ for $c \in \mathbf{Q}$.

(i) $L_1 = L_{67^3}$, $G_1 \cong G_{67^3} \cong S_3$.

$$F(1, 67^3; X) = -31f_1(X)f_2(X)f_3(X),$$

where

$$\begin{aligned} f_1(X) &= X - 5, \\ f_2(X) &= 98X^2 + 293X + 574, \\ f_3(X) &= 99X^3 - 197X^2 - 882X - 2843. \end{aligned}$$

We choose $u = 5$. It follows from (3) that $(x, y, z) = (134, 335, 201)$ and then

$$\begin{aligned} \text{Resultant}_X(X^3 + X + 1, \\ Y - (134 + 335X + 201X^2)) &= Y^3 + 67^3(Y + 1). \end{aligned}$$

Root fields of $f_2(X)$ and $f_3(X)$ give subfields of L_1 .

(ii) $L_1 \neq L_{63}$, $[L_1 \cap L_{63} : \mathbf{Q}] = 2$, $G_1 \cong G_{63} \cong S_3$.

There exists a cubic field M for which we have $\text{Spl}_M R(1; X) = \text{Spl}_M R(63; X)$. Indeed, in this case,

$$F(1, 63; X) = -31f_3^{(1)}(X)f_3^{(2)}(X)$$

where

$$\begin{aligned} f_3^{(1)}(X) &= X^3 - 3X^2 - 18X - 57, \\ f_3^{(2)}(X) &= 2X^3 - 3X^2 - 9X - 30. \end{aligned}$$

For each root field M of $f_3^{(1)}(X)$ or of $f_3^{(2)}(X)$ over \mathbf{Q} we have $\text{Spl}_M R(1; X) = \text{Spl}_M R(63; X)$.

(iii) $L_1 \neq L_2$, $L_1 \cap L_2 = \mathbf{Q}$, $G_1 \cong G_2 \cong S_3$.

$$\begin{aligned} F(1, 2; X) &= -X^6 + 35X^5 + 262X^4 \\ &\quad + 611X^3 - 1096X^2 - 801X - 1709 \end{aligned}$$

is irreducible over \mathbf{Q} .

(iv) $L_{-7} = L_{-49}$, $G_{-7} \cong G_{-49} \cong C_3$.

In this case, we have

$$F(-7, -49; X) = 7f_1^{(1)}(X)f_1^{(2)}(X)f_1^{(3)}(X)f_3(X)$$

where

$$\begin{aligned} f_1^{(1)}(X) &= X + 7, \\ f_1^{(2)}(X) &= 2X + 7, \\ f_1^{(3)}(X) &= 3X + 14, \\ f_3(X) &= X^3 + 13X^2 + 54X + 71. \end{aligned}$$

Take $u = -7, -7/2, -14/3$. Then we get $(x, y, z) = (14, 7, -3), (28, 7, -6), (-42, -14, 9)$, respectively, from (3). Using these (x, y, z) , we see

$$\begin{aligned} \text{Resultant}_X(X^3 - 7X - 7, Y - (x + yX + zX^2)) \\ = Y^3 - 49(Y + 1). \end{aligned}$$

(v) $L_{-7} \neq L_{-9}$, $G_{-7} \cong G_{-9} \cong C_3$.

$$F(-7, -9; X) = f_3^{(1)}(X)f_3^{(2)}(X),$$

where

$$\begin{aligned} f_3^{(1)}(X) &= X^3 + 21X^2 + 126X + 231, \\ f_3^{(2)}(X) &= 2X^3 + 21X^2 + 63X + 42. \end{aligned}$$

The splitting fields of $f_3^{(1)}(X)$ and of $f_3^{(2)}(X)$ give different cyclic cubic subfields of $L_{-7}L_{-9}$ which are also different from L_{-7} and L_{-9} .

5. Involutive Cremona transformation.

Let $K = k(s, t)$ be the rational function field in two variables s and t , and suppose that $\text{Spl}_M R(s; X) = \text{Spl}_M R(t; X)$ for an extension M of K . It follows from Theorem 1 that there exist $u, v \in M$ for which we have

$$t = \frac{s(u^2 + 9u - 3s)^3}{(u^3 - 2su^2 - 9su - 2s^2 - 27s)^2},$$

$$s = \frac{t(v^2 + 9v - 3t)^3}{(v^3 - 2tv^2 - 9tv - 2t^2 - 27t)^2}.$$

From this we also have

$$v = -\frac{(u^2 + 3s)(u^2 + 9u - 3s)}{u^3 - 2su^2 - 9su - 2s^2 - 27s}.$$

The correspondence $(s, u) \leftrightarrow (t, v)$ gives an involutive Cremona transformation σ over the field k . Let S and U be two independent variables over k ; then $\sigma \in \text{Cr}_2(k) = \text{Aut}_k(k(S, U))$ is given by

$$\sigma : (S, U) \mapsto \left(\frac{S(U^2 + 9U - 3S)^3}{(U^3 - 2SU^2 - 9SU - 2S^2 - 27S)^2}, \right. \\ \left. -\frac{(U^2 + 3S)(U^2 + 9U - 3S)}{U^3 - 2SU^2 - 9SU - 2S^2 - 27S} \right).$$

In contrast to the construction σ via Tschirnhausen transformation over k with $\text{ch}(k) \neq 3$, σ is defined over an arbitrary field k' . Indeed, over a field k' with $\text{ch}(k') = 3$, we have

$$\sigma : (S, U) \mapsto \left(\frac{SU^6}{(U^3 + SU^2 + S^2)^2}, \frac{2U^4}{U^3 + SU^2 + S^2} \right)$$

and $\sigma^2(S, U) = (S, U)$. Hence we regard S and U as independent variables over an arbitrary base field k' .

We study the rationality problem or the general Noether problem (cf. [7]) for $k'(S, U)^{(\sigma)}$ over k' . It is known as Zariski-Castelnuovo's theorem (cf. [17]) that if $k(S, U) \supset M \supseteq k$ with k algebraically closed of any characteristic and $k(S, U)$ is separable over M , then M is purely transcendental over k . However, this is not true for a general field. We show the rationality of $k'(S, U)^{(\sigma)}$ over an arbitrary field k' by constructing a minimal basis of $k'(S, U)^{(\sigma)}$.

Theorem 10. *Let k' be a field. The fixed field $k'(S, U)^{(\sigma)}$ of $k'(S, U)$ under the action of σ is purely transcendental over k' . If $\text{ch}(k') \neq 2$ then a minimal basis of $k'(S, U)^{(\sigma)}$ over k' is given by*

$$k'(S, U)^{(\sigma)} = \\ k' \left(\frac{2SU^3 + 9U^3 + 9SU^2 + 2S^2U + 54SU - 9S^2}{U^3 - 2SU^2 - 9SU - 2S^2 - 27S}, \right.$$

$$\left. \frac{S(4S + 27)(U^2 + 9U + S + 27)}{(2U + 9)(U^3 - 2SU^2 - 9SU - 2S^2 - 27S)} \right).$$

If $\text{ch}(k') = 2$ then

$$k'(S, U)^{(\sigma)} = k' \left(\frac{U^3 + SU^2 + S^2}{U^3 + SU + S}, \frac{S}{U^3 + SU + S} \right).$$

Proof. Put $L := k'(S, U)$ and $\sigma = \sigma_1\sigma_2$, where

$$\sigma_1 : (S, U) \mapsto \left(\frac{S(U^2 + 9U - 3S)^3}{(U^3 - 2U^2S - 9SU - 2S^2 - 27S)^2}, U \right),$$

$$\sigma_2 : (S, U) \mapsto \left(S, -\frac{(U^2 + 3S)(U^2 + 9U - 3S)}{U^3 - 2SU^2 - 9SU - 2S^2 - 27S} \right).$$

We define

$$(4) \quad (x, y) := (\text{Tr}_\sigma(S), \text{Tr}_\sigma(U)) \\ = (S + \sigma_1(S), U + \sigma_2(U)).$$

First we assume $\text{ch}(k') \neq 2$. Then we can show

$$(5) \quad L^{\langle \sigma_1 \rangle \times \langle \sigma_2 \rangle} = k'(x, y).$$

Indeed, it follows from the definition of (x, y) that $L^{\langle \sigma_1 \rangle \times \langle \sigma_2 \rangle} \supset k'(x, y)$. Then by using computer manipulation we obtain the following equations:

$$486S - 36S^2 - 243x + 54xS + 729y + 270yS \\ - 54xy + 4xyS + 243y^2 + 54y^2S + 18y^3 \\ + 4y^3S - 2U(729 + 54S + 4S^2 + 54x - 2xS \\ + 243y + 18yS + 9xy + 27y^2 + 2y^2S + y^3) = 0,$$

$$16S^4 - 32xS^3 + 4S(S - x)(1458 + 135x + 5x^2 \\ + 729y + 36xy + 162y^2 + 2xy^2 + 20y^3 + y^4) \\ + 16x^3S - (3x - 9y - y^2)^3 = 0.$$

From the first equation we have $U \in k'(x, y)(S)$ because it is linear in U and $\text{ch}(k') \neq 2$. By the second equation, we have $k'(S, U) = k'(x, y)(S)$ and $[k'(S, U) : k'(x, y)] = 4$. Hence we conclude the equality of (5). Now we have $L^{(\sigma)} \supset k'(x, y)$ and $[L^{(\sigma)} : k'(x, y)] = 2$. Next we put

$$(6) \quad z := \frac{S - \sigma_1(S)}{U - \sigma_2(U)}.$$

Then we see x, y, z satisfy

$$81 + 9x + 18y + xy + y^2 \\ + xz - 9yz - y^2z - 9z^2 - yz^2 = 0.$$

Hence, we conclude $L^{(\sigma)} = k'(y, z)$ because we have $L^{(\sigma)} \supset k'(x, y)(z)$, $[k'(x, y)(z) : k'(x, y)] = 2$ and

$k'(x, y, z) = k'(y, z)$. Finally we can compute y, z directly from the definition as

$$y = -\frac{2SU^3 + 9U^3 + 9SU^2 + 2S^2U + 54SU - 9S^2}{U^3 - 2SU^2 - 9SU - 2S^2 - 27S},$$

$$z = -\frac{S(4S + 27)(U^2 + 9U + S + 27)}{(2U + 9)(U^3 - 2SU^2 - 9SU - 2S^2 - 27S)}.$$

Next we assume $\text{ch}(k') = 2$. In this case, σ is described as

$$\sigma : (S, U) \mapsto \left(\frac{S(U^2 + U + S)(U^4 + U^2 + S^2)}{U^6 + S^2U^2 + S^2}, \frac{U^4 + U^3 + SU + S^2}{U^3 + SU + S} \right).$$

From a similar way as above we see that

$$x + y + y^2 = 0, \quad z = \frac{x}{y},$$

where x, y, z are defined as in (4) and (6). Thus we have $k'(x, y, z) = k'(y)$ and

$$y = U + \sigma(U) = \frac{U^3 + SU^2 + S^2}{U^3 + SU + S}$$

in the case of $\text{ch}(k') = 2$. Now we put

$$w := \frac{S}{U} + \frac{\sigma(S)}{\sigma(U)} = \frac{S(U^3 + SU^2 + S^2)}{U(U^5 + SU^2 + S^2U + S^2)}.$$

Then we obtain $k'(S, U)^{(\sigma)} = k'(y, w)$ as follows: From the definition of y and w , we have $k'(S, U)^{(\sigma)} \supset k'(y, w)$. We put

$$W := \frac{w}{y + w} = \frac{S}{U^3 + SU + S}.$$

Then $k'(y, w) = k'(y, W)$ and we see that y, W, S, U satisfy

$$S + yU + U + W + y + 1 = 0,$$

$$WU^2 + yWU + W^2 + yW + y + 1 = 0.$$

Hence the equality $k'(S, U)^{(\sigma)} = k'(y, W) = k'(y, w)$ follows from $k'(S, U) = k'(y, W)(U)$ and $[k'(S, U) : k'(y, W)] = 2$. \square

The calculations in this paper were carried out with Mathematica [16].

References

- [1] E. Bertini, Ricerche sulle trasformazioni univoche involutorie nel piano, *Annali di Mat.* **8** (1877), 244–286.
- [2] L. Bayle and A. Beauville, Birational involutions of \mathbf{P}^2 , *Asian J. Math.* **4** (2000), no. 1, 11–17.
- [3] A. A. Bruen, C. U. Jensen and N. Yui, Polynomials with Frobenius groups of prime degree as Galois groups. II, *J. Number Theory* **24** (1986), no. 3, 305–359.
- [4] G. Butler and J. McKay, The transitive groups of degree up to eleven, *Comm. Algebra* **11** (1983), no. 8, 863–911.
- [5] G. Castelnuovo and F. Enriques, Sulle condizioni di razionalità dei piani doppi, *Rend. del Circ. Mat. di Palermo* **14** (1900), 290–302.
- [6] K.-I. Hashimoto and K. Miyake, Inverse Galois problem for dihedral groups, in *Number theory and its applications (Kyoto, 1997)*, 165–181, Kluwer Acad. Publ., Dordrecht, 1999.
- [7] C. U. Jensen, A. Ledet and N. Yui, *Generic polynomials*, Cambridge Univ. Press, Cambridge, 2002.
- [8] G. Kemper, Generic polynomials are descent-generic, *Manuscripta Math.* **105** (2001), no. 1, 139–141.
- [9] Y. Kishi and K. Miyake, Parametrization of the quadratic fields whose class numbers are divisible by three, *J. Number Theory* **80** (2000), no. 2, 209–217.
- [10] T. Komatsu, Arithmetic of Rikuna’s generic cyclic polynomial and generalization of Kummer theory, *Manuscripta Math.* **114** (2004), no. 3, 265–279.
- [11] T. Komatsu, Generic sextic polynomial related to the subfield problem of a cubic polynomial. (Preprint). <http://www.math.kyushu-u.ac.jp/coe/report/pdf/2006-9.pdf>
- [12] A. Ledet, On groups with essential dimension one, *J. Algebra.* (to appear).
- [13] M. D. Miller, On the lattice of normal subgroups of a direct product, *Pacific J. Math.* **60** (1975), no. 2, 153–158.
- [14] K. Miyake, Twists of Hessian Elliptic Curves and Cubic Fields, in *The Proceedings of Congrès International, Algèbre, Théorie des nombres et leurs Applications*, Université Mohammed I, Oujda-Saidia, Maroc, 2006. (to appear).
- [15] K. Miyake, Two Expositions on Arithmetic of Cubics, in *The Proceedings of The Fourth China-Japan Conference on Number Theory*, Shandong University Academic Center, Weihai, 2006. (to appear).
- [16] S. Wolfram, *The Mathematica® book*, Fourth edition, Wolfram Media, Inc., Champaign, IL, 1999.
- [17] O. Zariski, On Castelnuovo’s criterion of rationality $p_a = P_2 = 0$ of an algebraic surface, *Illinois J. Math.* **2** (1958), 303–315.